K.Balaji* et al.
(IJITR) INTERNATIONAL JOURNAL OF INNOVATIVE TECHNOLOGY AND RESEARCH
Volume No.2, Issue No. 4, June – July 2014, 1049 – 1053.
Research Article

A Key Based Data Sharing Protocol for Secure Inter Group Transfers

K .BALAJI
Associate Professor
Dept of IT
Dadi Institute Of Engineering & Technology
Anakapalli

K NUKARAJU
Associate Professor
Dept of IT
Dadi Institute Of Engineering & Technology
Anakapalli.

Abstract:- **Storing data on remote cloud storage makes the maintenance affordable by data owners. The reliability and trustworthiness of these remote storage locations is the main concern for data owners and cloud service providers. When multiple data owners are involved, the aspects of membership and data sharing need to be addressed. In this paper the authors proposed efficient multi owner data sharing technique over cloud storage. The proposed scheme provides privacy and complexity while handling the data sharing over cloud. The proposed technique works with improved Shamir's secret sharing group key mechanism. In this technique data can be uploaded in to the server after the encryption of the content by the secret group key. When new member joined in the group, new granted users can directly decrypt data files uploaded without contacting with data owners.**

Keywords: **Data Sharing, Cloud Computing, Access Control, User Revocation.**

I. INTRODUCTION

With cloud computing and storage, users are able to access and to share resources offered by cloud service providers at a lower marginal cost. With Dropbox, for example, data is stored in the cloud (operated by Amazon), and shared among a group of users in a collaborative manner. It is natural for users to wonder whether their data remain intact over a prolonged period of time. The Privacy of data stored in the cloud can become compromised. To protect the privacy of data in the cloud and to offer "peace of 653mind" to users, it is best to encrypt the data files and then upload the encrypted data into the cloud [2]. Unfortunately designing an efficient and secure data sharing scheme for groups in the cloud is not an easy task due to following reasons. First, the identity of the data owners must be preserved. Second, the data owner should be able to utilize all the services provided by the cloud storage service provider [3].

Many privacy techniques for data sharing on remote storage machines have been recommended [4],[5], [6]. In these models, the data owners store the encrypted data on untrusted remote storage. After that they will share the respective decryption keys with the authorized users. This prevent the cloud service providers and intruders to access the encrypted data, as they don't have the decrypting keys. However the new data owner registration in the above said models reveals the identity of the new data owner to the others in the group. The new data owner has to take permission from other data owners in the group before generating a decrypting key. The proposed system identified the problems during multi owner data sharing and proposed an efficient protocol and cryptographic technique for solving drawbacks in the traditional approach. It proposed an efficient and novel secure key protocol for group key generation and using these key data owners can encrypt the files. Suppose new user register into group the user need not to contact the data owner during the downloading of files and data can be encrypted with AES before uploading the data in to the cloud.

II. RELATED WORK

In [1], the authors specified a secure data sharing model, Mona, for dynamic groups in a remote storage. In Mona, a data owner can share data with others in the group without announcing their identity.

Moreover, Mona supports effective user repudiation and new user registration. More specially, efficient user repudiation can be attained by a public revocation list without ideating the private keys of the remaining users, and new users can directly decrypt files stored in the cloud before their presence.

In [4], Kallahalla et al. developed a cryptographic storage system that facilitates secure file sharing on untrusted servers. By breaking files into filegroups and encrypting each filegroup with a exclusive file-block key, the data owner can share the filegroups with others by handover of the corresponding lockbox key. In fact, it gives an additional load for key distribution. Apart from this, the file-block key needs to be renewed and delivered again for a user revocation.

In [5], the contents of files placed on remote server are metadata and file data. The file metadata

contains the access control data that encompass collection of encrypted keys. These metadata files are encrypted with public key of authorized users. As the file metadata should be refurbished, the user abrogation in the scheme is an uncompromising issue particularly for large-scale sharing. Nonetheless, the private key should be regenerated for each user for every new user addition into the group. This limits the application to support dynamic groups. Another issue is the encryption load enhances with the sharing scale. .

The proxy reencryption model given by Ateniese et al. [6] strengthens the distributed storage. The data encryption done by the data owners is a two step procedure. First, encryption is done using exclusive and symmetric content keys. Second, the data is encrypted with a master public key. Proxy cryptography is used by the server to reencrypt the particular content key(s) from the master public key. On the other hand, the remote storage server can be attacked by any malicious user to find the decryption keys of all encrypted blocks.

From the above analysis, the authors observed that how to securely share data files in a multiple-owner manner for dynamic groups while preserving identity privacy from an untrusted cloud remains to be a challenging issue. In this paper, the authors proposed a novel multi owner data sharing group key protocol for secure data sharing in cloud computing.

III. SYSTEM MODEL AND DESIGN GOALS

3.1 System Model

The system model consists of three different entities: as illustrated in below Figure, the cloud, a group manager (i.e., the company manager), and a large number of group members (i.e., the staffs) .Cloud is operated by CSPs and provides priced abundant storage services. However, the cloud is not fully trusted by users since the CSPs are very likely to be outside of the cloud users' trusted domain.

Group manager takes charge of system parameters generation, user registration, user revocation, and revealing the real identity of a dispute data owner.

Group members are a set of registered users that will store their private data into the cloud server and share them with others in the group.

Figure System model.

3.2 Design Goals

In this section, I describe the main design goals of the proposed scheme including access control, data confidentiality, anonymity and traceability, and efficiency as follows:

3.2.1 Access control:

The requirement of access control is twofold. First, group members are able to use the cloud resource for data operations. Second, unauthorized users cannot access the cloud resource at any time, and revoked users will be incapable of using the cloud again once they are revoked.

3.2.2 Data confidentiality:

Data confidentiality requires that unauthorized users including the cloud are incapable of learning the content of the stored data. An important and challenging issue for data confidentiality is to maintain its availability for dynamic groups. Specifically, new users should decrypt the data stored in the cloud before their participation, and revoked users are unable to decrypt the data moved into the cloud after the revocation.

3.2.3 Anonymity and traceability:

Anonymity guarantees that group members can access the cloud without revealing the real identity. Although anonymity represents an effective protection for user identity, it also poses a potential inside attack risk to the system.

3.2.4 Efficiency:

The efficiency is defined as follows: Any group ember can store and share data files with others in the group by the cloud. User revocation can be achieved without involving the remaining users. . That is, the remaining users do not need to update their private keys or re-encryption operations. New granted users can learn all the content data files stored before his participation without contacting with the data owner.

IV. PROPOSED WORK

The proposed system identified the problems during multi owner data sharing and proposed an efficient protocol and cryptographic technique for solving drawbacks in the traditional approach. It proposed an efficient and novel secure key protocol for group key generation. In this system new user need not to contact the data owner during the downloading of files and data can be encrypted with AES before uploading the data in to the cloud.

4.1 Data owner

Data owner requires registration before uploading the data in to the service. Data owner can upload the data into the service after encrypting the file by the key which is generated by the group key manager. Data owner can download the content when ever required.

4.2 Group key manager

Group key manger receives the registration request from all the users, and generates a verification share and forwards to all the requested users for authentication purpose. Group key manager generates the key using key generation process and forwards the points to extract ion of the key from the equation generated by the verification points.

For key generation protocol, Group key manager receives the verification shares and key as input to construct the Lagrange's polynomial equation f(x), which is passed, through (0, key) and verification points. After that group key manager forwards the points to data owners. Data owners again reconstruct the key from the verification points and check the authentication code which is sent by the group key manager.

When a new user tries to download the file, new user need not connect with other data owners. For decryption of the file new user connects to the group key manager then group key manager will update the group key and decrypts the files with previous key again encrypt with new key and updates the new key to all the data owners.

Data owner initiate the request by sending the random challenge to the group key manager, as a response Group key manager sends a secret share. Data owner authenticates and forwards the verification share. Group key manager receives the verification shares and generates the key using Lagrange's polynomial equation and forwards the points to data owners for regenerating the key.

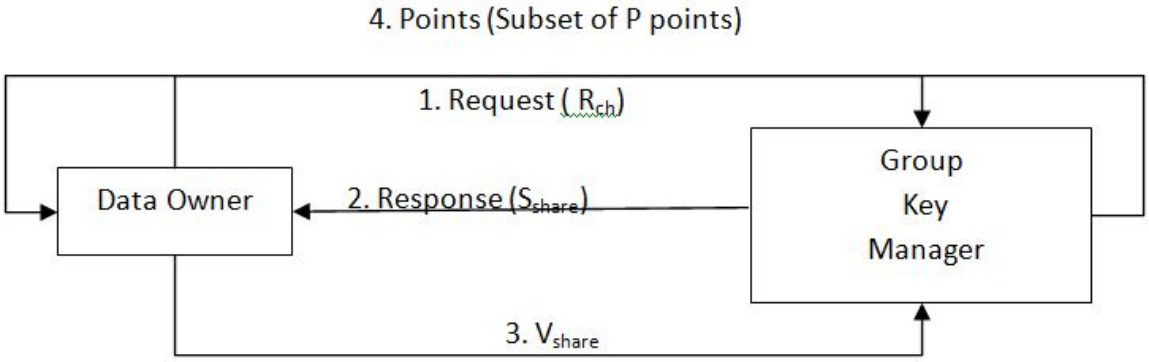


Figure: Initiation process

R_{ch} ----Random challenge

S_{share}---Secret share

V_{share}----verification share

P= $\{p_1, p_{2...} p_n\}$----------points for construction of Lagrange's equation

4.3 *Out sourcing of data over service*

Data owner reads the required file content and encrypts the file with key, which is generated by the group key manager. For encryption of the data, the proposed system uses AES algorithm for encryption of the file and uploads in to the server. Data owner can download the file when ever required.

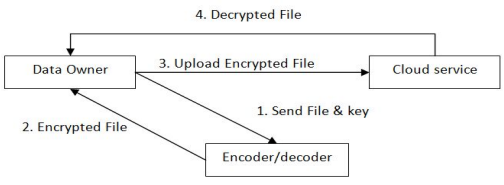


Figure: ***Out sourcing of data***

4.4 User Revocation

Whenever new user tries to download the file, new user need not consult all the data owners. New user can be revoked by the group key manager in regular registration process. Group key manager updates the key, decrypts the data file with old key and encrypts with the new key and forwards the key to the all the related data owners.

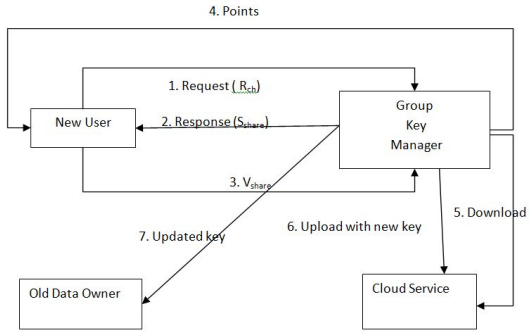
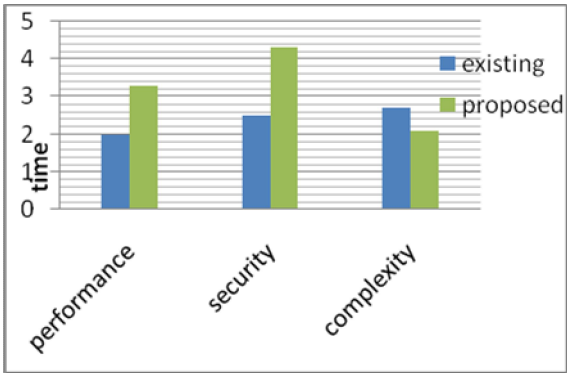


Figure: ***User Revocation***

V. PROPOSED MODEL EVALUATION

In this section I present the performance report of our proposed model with the existing model. The below graph describes the performance, security and complexity attributes of the proposed model.



5.1 Performance:

The performance of proposed system is more compare to existing one, because in proposed system if new user enters into the cloud he does not depend on other users. The new user directly communicates with the group key manager and getting secret key. So the performance of the proposed system is high.

5.2 Security:

The security of proposed system is high compare to existing one. Since the group members only know the secret key. Suppose an unknown person enter into group he does not find the secret key i.e. the user enters into group confirm that he must be a group member.

5.3 Complexity:

The complexity of proposed system is low compare to existing one. Because the new user does not worry about getting the secret key i.e. the new user does not depend on the remaining group members. The new user directly communicates with group key manager and gets the secret key. The encryption and decryption of file also take less time.

VI. CONCLUSION

In this paper, I developed a secure Multi owner Data sharing Group key protocol for an untrusted cloud. In this model, a new user can store data on the cloud storage without communicating with all the data owners. The group key manager grants the key on request to the new data owners directly. The new user revocation and registration is made simple by allowing the user to communicate with the group key manager through the revocation policy. The storage overhead and the encryption computation cost are varied.

REFERENCES

[1] Xuefeng Liu, Yuqing Zhang, Member, IEEE, Boyang Wang, and Jingbo Yan Xuefeng Liu, Yuqing Zhang, Member, IEEE, Boyang Wang, and Jingbo Yan, Ieee transactions on parallel and distributed systems, vol. 24, no. 6, june 2013

[2] S. Kamara and K. Lauter, "Cryptographic Cloud Storage," Proc. Int'l Conf. Financial Cryptography and Data Security (FC), pp. 136-149, Jan. 2010.

[3] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable,and Fine-Grained Data Access Control in Cloud Computing,"Proc. IEEE INFOCOM, pp. 534-542, 2010.

[4] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu,"Plutus: Scalable Secure File Sharing on Untrusted Storage," Proc.USENIX Conf. File and Storage Technologies, pp. 29-42, 2003.

[5] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing Remote Untrusted Storage," Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 131-145, 2003.

[6] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage," Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 29-43, 2005.

[7] Boneh, D., Boyen, X., Shacham, H.: Short Group Signatures. In: Proc. CRYPTO. pp. 41–55. Springer-Verlag (2004)

[8] Boneh, D., Freeman, D.M.: Homomorphic Signatures for Polynomial Functions. In: Proc. EUROCRYPT. pp. 149–168. Springer-Verlag (2011)

[9] Boneh, D., Gentry, C., Lynn, B., Shacham, H.: Aggregate and Verifiably Encrypted Signatures from Bilinear Maps. In: Proc. EUROCRYPT. pp. 416–432. SpringerVerlag (2003)

[10] Boneh, D., Lynn, B., Shacham, H.: Short Signatures from the Weil Pairing. In: Proc. ASIACRYPT. pp.514–532. Springer-Verlag (2001)

[11] Chaum, D., van Heyst, E.: Group Signatures. In: Proc.EUROCRYPT.pp.257–265.Springer-Verlag (1991).

